修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院　情報システム学研究科　　情報ネットワーク学専攻　博士前期課程		
氏　　名	森川　敬介	学籍番号	0651029
論 文 題 目	Peres 型乱数変換に関する研究		

要　　旨

乱数を発生させる方法は様々あるが，本研究では分布に偏りのある非一様乱数から偏りのない一様乱数を取り出すような乱数変換を考え，この乱数変換いう立場から議論した．

1951 年，von Neumann は出現確率が未知，離散アルファベットが 2 値である i.i.d. 系列から偏りの無い乱数列を作る考え方を示した．これは 2 ビットずつ入力系列を比較し，01,10 の時のみを 0,1 と変換し出力する考え方である．しかし，この手順は入力長に対して出力が少なく，必ずしも変換効率の良いアルゴリズムではなかった．1972 年，P.Elias が同じハミング重み（入力長の中の 1 の個数）の系列における出現確率に着目し，一様な乱数列を取り出す方法を提案した．この方法では入力系列を十分大きく取ると，平均符号長がエントロピーまで漸近することを示されている．その後，1993 年，Y.Peres が von Neumann 法の拡張(以下，2 値 Peres 法と呼ぶ)を提案した．この方法では von Neumann 法に別の変換を組合せ，繰り返し適用することで多くの乱数列を取り出すことを可能とした．そして，Elias 法と同様，十分大きな入力系列に対して入力長に対する出力長の割合がエントロピーまで漸近することが示されている．

本研究ではまず 2 値 Peres 法の実装を行い，その後，Elias 法，Lynch-Davisson 符号との比較を行なった．Lynch-Davisson 符号とは，Elias 法と非常に近い手順を用いるが乱数変換ではなく，データ圧縮のための符号化である．また，Lynch-Davisson 符号も十分大きな入力系列に対して平均符号長がエントロピーに漸近することが知られている．この 2 つの方法と比較し，2 値 Peres 法に対する特性，性質を調べた．結果として，2 値 Peres 法は Elias 法と比べ変換効率の面で劣っている事が確認できた．そこで，乱数変換という点で 2 値 Peres 法，Elias 法で最も異なっているのが入力系列に対する処理と考え，切り捨てビットに着目した．切り捨てビットとは，von Neumann 法，2 値 Peres 法において，2 ビットずつ比較するために入力系列が奇数列の場合 1 ビット切り捨てて偶数列にした時のビット数の事をいう．この 1 ビットの切り捨てについても議論した．

さらに，Peres 法の入力アルファベットを 3 値に拡張し，3 値の系列を 2 値の偏りの無い乱数列に変換する「3 値 Peres 法」について考察し，実装を行った．そして，出力系列に対して乱数検定を行い，偏りの無い乱数としての性質を満たしていることを確認した．